

## Quantum Computers, Factoring and Decoherence

I. L. Chuang<sup>1</sup>, R. Laflamme<sup>2</sup>, P. Shor<sup>3</sup> and W. H. Zurek<sup>2</sup><sup>1</sup> Edward L. Ginzton Laboratory, Stanford University, Stanford, CA, 94305, USA<sup>2</sup>Theoretical Astrophysics, T-6, MS B288

Los Alamos National Laboratory, Los Alamos, NM87545, USA

<sup>3</sup>AT& T Bell Labs, 600 Mountain Ave., Murray Hill, NJ 07974, USA

February 5, 1995

**Abstract**

In a quantum computer any superposition of inputs evolves unitarily into the corresponding superposition of outputs. It has been recently demonstrated that such computers can dramatically speed up the task of finding factors of large numbers – a problem of great practical significance because of its cryptographic applications. Instead of the nearly exponential ( $\sim \exp L^{1/3}$ , for a number with  $L$  digits) time required by the fastest classical algorithm, the quantum algorithm gives factors in a time polynomial in  $L$  ( $\sim L^2$ ). This enormous speed-up is possible in principle because quantum computation can simultaneously follow all of the paths corresponding to the distinct classical inputs, obtaining the solution as a result of coherent quantum interference between the alternatives. Hence, a quantum computer is sophisticated interference device, and it is essential for its quantum state to remain coherent in the course of the operation. In this report we investigate the effect of decoherence on the quantum factorization algorithm and establish an upper bound on a “quantum factorizable”  $L$  based on the decoherence suffered per operational step.

The uniqueness of the prime factorization of a positive integer is the Fundamental Theorem of Arithmetic[1]. However, in practice, the determination of the prime factors of a given number can be an exceedingly difficult problem, although verification is trivial. This asymmetry is the basis for modern cryptography, and provides secret codes used not only on your own bank card but also to transfer diplomatic messages between embassies.

Attempts to undermine the security provided by the difficulty of factorization have met with failure by and large, even with the aid of powerful modern computers. In fact, this problem is widely believed to have no polynomial-time algorithm[2], although a proof of this statement has remained elusive. The best known classical computer algorithm[3] to factor a number  $N$  of  $L$  digits takes a time exponential in  $L^{1/3}$ .

In contrast, one of us[4] has shown recently that with the help of a quantum computer one can factor numbers in a random *polynomial* amount of time. Therefore these new computers could be a threat to what is presently the most common method of encrypted message transfer. However, it is still unknown whether such machines are *practical*, because they depend crucially

on quantum-mechanical behavior which is uncommon to our mostly classical world. This issue is one of decoherence[5], the subject of our study.

The quantum factoring algorithm uses in an essential way the coherence of a quantum wavefunction. In a nutshell, to factor a number  $N$  one chooses a number  $x$  at random and calculates its order  $r$  modulo  $N$ , i.e. finds  $r$  such that  $x^r \equiv 1 \pmod{N}$ . Once  $r$  is known, factors of  $N$  may often be found using the Chinese remainder theorem. The difficulty is to calculate  $r$ . The quantum factoring algorithm goes as follows. First choose a smooth number (one with small prime factors)  $q$  such that  $N^2 < q < 2N^2$  and build the state;

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle, \quad (1)$$

from which can be obtained (using a quantum computer)

$$|\psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \pmod{N}\rangle. \quad (2)$$

We can now Fourier transform this pure state (again using a quantum computer) to get;

$$|\psi_3\rangle = \frac{1}{q} \sum_{c=0}^{q-1} \sum_{a=0}^{q-1} e^{i2\pi ac/q} |c, x^a \pmod{N}\rangle, \quad (3)$$

and measure both arguments of this superposition, obtaining  $\bar{c}$  for the first one and some  $x^k$  as the answer for the second one ( $k$  being any number between 0 and  $r$ ). Given the pure state  $|\psi_3\rangle$ , probabilities of different results for this measurement will be given by the probability distribution;

$$P(\bar{c}, x^k) = \left| \frac{1}{q} \sum_{a=0}^{q-1} e^{i2\pi a\bar{c}/q} \right|^2, \quad (4)$$

where the prime indicates a restricted sum over values of  $a$  which satisfy  $x^a \equiv x^k \pmod{N}$ . This function has periodicity  $q/r$ , but as we know  $q$ , we can determine  $r$  with a few trial executions (an example is shown in Fig. 1). A measurement thus gives with high probability  $c = \lambda q/r$ , where  $\lambda$  is an integer which corresponds to a particular peak in Fig. 1. With a few runs of the program, we can deduce  $r$  and thus the factors of  $N$ .

The algorithm discussed above assumes that the quantum computer was completely isolated. In practice this will certainly not be the case. It is the effect of imperfect isolation which we study here. A first obvious effect is that the quantum computer will lose energy. This happens at the rate  $\tau_{rel}$ , the relaxation time-scale. It is relatively easy to make systems for which  $\tau_{rel}$  can be very large and thus allow a reasonable number of operation to complete. A much more insidious effect of imperfect isolation is *decoherence*[5]. Decoherence is caused by the continuous

interaction between the system (in our case the quantum computer) and the environment[5-7]. As a result, the state of the environment “monitors,” and therefore becomes correlated with, the state of the system. As a quantum system evolves, information about its states leaks out into the environment, causing them to lose their purity, and, consequently, their ability to interfere.

It is important to realize that the timescale for decoherence  $\tau_{dec}$  is much smaller than the one for relaxation. For example, an oscillator of mass  $m$  in a superposition of coherent states (separated by a distance  $\Delta x$  from each other) interacting linearly with a bath at temperature  $T$  has the decoherence time[7]

$$\tau_{dec} \sim \tau_{rel} \left[ \frac{\lambda_{dB}}{\Delta x} \right]^2, \quad (5)$$

where  $\lambda_{dB}$  is the thermal de Broglie wavelength. This expression is valid for high temperatures only; at low temperatures, the  $\tau_{dec}$  becomes inversely proportional to the cut-off frequency of the bath. It is crucial to realize that no net energy transfer is needed to effect decoherence. This implies a much greater sensitivity of quantum computation to decoherence than to the relaxation process.

The decoherence process has been proposed as a mechanism for enforcing classical behavior in the macroscopic realm. Decoherence results in environment-induced superselection[5, 6, 7] which destroys superpositions between the states of preferred pointer basis[6]. Classical computers are already decohered – computation takes them through a predictable sequence of such pointer states, which are stable in spite of the environment. Thus, classical computers cannot be put in arbitrary superpositions and cannot take advantage of the quantum factoring algorithm. But coupling with the environment will also be inevitable for any system employed to implement the quantum factoring algorithm. Here, we will show what the effect of decoherence on the quantum factoring algorithm is.

Our model involves the introduction of the environment as a system external to the computer. Its state is represented by third label. The input state may thus be written as

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle \times |\epsilon\rangle, \quad (6)$$

where  $\epsilon$  are the degrees of freedom of the environment. The environment is initially uncorrelated with the computer; however, it is likely that the interaction between bits necessary for the calculation of  $x^a \bmod N$  will involve some interaction with the environment, so that the next state,

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod N\rangle \times |\epsilon_a\rangle, \quad (7)$$

leaves the environment partially correlated with the state of the computer. Now, if the physical representation for the computer’s quantum bits is diagonal in the pointer basis of the environ-

ment, then decoherence results in no adverse effects when measuring the second label of  $|\tilde{\psi}_2\rangle$ . Such a design would be optimal. We thus focus on the effects of decoherence on the first label, by suppressing the second label, and tracing over the environment to obtain the reduced density matrix;

$$\rho_{red} = \frac{1}{q} \sum_{a=0}^{q-1} \sum_{a'=0}^{q-1} [1 - \beta_{aa'}] |a\rangle\langle a'|. \quad (8)$$

Here  $1 - \beta_{aa'} = |\langle \epsilon_a | \epsilon_{a'} \rangle|^2$  is a measure of the accuracy with which the state of the environment has become correlated with the state of the quantum computer. If  $|a\rangle$  and  $|a'\rangle$  are quantum bit register states diagonal in the pointer basis, then we may take;

$$1 - \beta_{aa'} \approx \exp \left[ -\xi(a \otimes a') \right], \quad (9)$$

where  $\otimes$  is defined as the exclusive-or (XOR) function, and gives the Hamming distance[8] between  $a$  and  $a'$ .  $\xi$  is a constant parameter which depends on the particular realization of the quantum computer. The measurement results in a probability distribution, shown in Fig. 2, which differs from the one in eq. (4) (see Fig. 1) in that non-zero-probabilities have appeared between the peaks and that these peaks have decreased in amplitude.

The qualitative effect of decoherence is well approximated by the simpler function  $1 - \beta_{aa'} \equiv \delta_{aa'} + (1 - \delta_{aa'})\beta$ , where  $\beta$  is a constant. For  $\beta = 0$  we get the state with complete coherence and  $\beta = 1$  one with complete decoherence (i.e., a matrix diagonal in the pointer state). In the limit of  $\beta \sim 1$ , we may understand  $\beta$  using the fractional amount of *information lost to the environment*, expressed as  $S_f/S_{max} = 1 - (1 - \beta)^2$ , where  $S_{max}$  is the entropy of a completely decohered computer and  $S_f$  is the difference between the entropy of the final state of the computer and the one from the initial state (assumed to be nearly zero). For  $\beta \approx 0.5$  the probability between the peaks (see Fig. 2) is equal to the one of the peaks, and thus there is as much chance to get a correct answer than a wrong one. Once  $(1 - \beta)^{-1} \sim \mathcal{O}(\exp[(\log N)^{1/3}])$ , the quantum computer becomes as inefficient as a classical one. In this case it would take a number of trials exponential in  $(\log N)^{1/3}$  in order to factor the number  $N$ .

In principle it is easy to calculate  $\beta$  from an experiment. If we allow the input to be in the superposition  $|\uparrow_{in}\rangle + |\downarrow_{in}\rangle$  then the coefficient  $\beta$  is given by

$$\beta = 1 - \frac{\rho_{\uparrow\downarrow}^{out} + \rho_{\downarrow\uparrow}^{out}}{\rho_{\uparrow\uparrow}^{out} + \rho_{\downarrow\downarrow}^{out}}. \quad (10)$$

In a two slit experiment, it is the ratio between the amplitude of the destructive and constructive interference on the screen also called the fringe visibility function.

It is reasonable to assume, to first approximation, that the loss of coherence is linear with the number of operations in the computation. This is equivalent to saying that the environment keeps no memory of the system as it evolves from one step to another. Thus  $1 - \beta \approx n_{op}\alpha$ ,

where  $\alpha$  is the coherence lost in a simple operation (once coherence is lost in such systems it cannot be regained). When  $\alpha$  is small it can also be interpreted as the fractional information loss per operation, i.e. such that  $\Delta S/S_{max} = \alpha$ .  $n_{op}$  is the operation count,  $n_{op} \sim [\log N]^2$ . It is therefore possible to estimate the total loss of quantum coherence by studying only one part of the computer. To factor a number  $N$  the quantum algorithm uses  $\mathcal{O}([\ln N]^2)$  operations and therefore  $\alpha^{-1} \sim \mathcal{O}([\ln N]^2)$ . The quantum computer allows a significant amount of decoherence. One of the reasons is that factoring is in the class of the so-called NP functions, i.e. functions which are hard to solve but once the answer is known it is fairly easy to verify. The quantum computer can therefore run until we find the correct factors.

How much entropy is lost to the environment per step? Designs for quantum computers have been suggested[9, 10, 11, 12] and some possible difficulties investigated[13, 14]. Common to these designs is the model of a simple two state system interacting with an ensemble of oscillators (the environment), from which we can get an idea for what  $\alpha$  is. We use as a Hamiltonian

$$H = \frac{\Delta}{2} \hat{\sigma}_x + \mu \hat{\sigma}_z \sum_n C_n q_n + \sum_n h_n. \quad (11)$$

where the  $\sigma$ 's are Pauli matrices,  $q_n$  are the coordinates of the environment oscillators and  $h_n$  are harmonic oscillator Hamiltonians (a cutoff  $\Lambda$  is implicit). It can be seen that without the environment, a state of the system of the form  $|\uparrow\rangle$  turns into the state  $(|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$  in a time  $\pi/2\Delta$ . This is a typical step for a quantum computer.

Thus, the effect of a zero temperature environment is to decrease the off-diagonal term of the density matrix by the amount[15]

$$\alpha \sim \frac{\mu^2 \eta}{2\pi} \left[ -\mathbf{C} - \frac{\pi^2}{4} + \log \left( \frac{\Delta}{\Lambda} \right) \right]. \quad (12)$$

Here,  $\mathbf{C}$  is Euler's constant and  $\eta$  is the viscosity coefficient determined by the spectral density of the oscillators. A non-zero temperature will further increase the value of  $\alpha$ .

With perfect operation, each execution trial gives a factor of  $N$  with probability  $\mathcal{O}(\log N)$ , but with decoherence, the number of trials required becomes  $\mathcal{O}(\log N/(1 - \beta))$ . In terms of  $\alpha$ , we find that with decoherence, the required number of executions of the quantum algorithm to find a factor of  $N$  is of order

$$\text{Number of trials} \sim \frac{L}{1 - L^2 \alpha}, \quad (13)$$

where  $L = \log N$ . To give performance better than the classical algorithm, we must therefore have that

$$\frac{L}{1 - L^2 \alpha} \leq \exp [L^{1/3}]. \quad (14)$$

Using eq (12) and (14) we find that the largest number which can be factored efficiently

with a quantum computer is

$$N \sim \exp \left[ \frac{1}{\sqrt{\alpha}} \right] \sim \exp \left[ \sqrt{\frac{2\pi}{\mu^2 \eta}} \right]. \quad (15)$$

The quantum algorithm to factor numbers uses the quantum computer as a huge interferometer. When it is perfectly isolated, the interference fringes give the important clue to the factors. When isolation is not perfect anymore there are chances that the result is irrelevant for factoring. The quantum computer is efficient as long as we can discover the interference pattern in a number of trials less than the one given by the classical algorithm.

Many are skeptical of the possibility of building useful quantum computers. This attitude is largely fuelled by the inevitability of decoherence and the fragility of the information encoded in coherent quantum superposition[13, 14]. In particular, error correction which ensures reliability of classical computers may be very difficult to accomplish quantum mechanically. We note that these critical remarks, while well taken, are based on a classical paradigm: Computers are useful when they always (or almost always) get right answers. By contrast, as a result of decoherence quantum computers will often give wrong answers. However, providing that the resulting probability distribution still gives one a clue of what the right answers are, quantum computers will be useful. This is because for one-way functions (which form a substantial class of NP-hard problems) verification is trivial. Thus a probability distribution emerging from a quantum computer may suffice: Fringes in an interference experiment allow one to identify the characteristic frequency of a source even when the contrast is far from perfect.

### Acknowledgment.

We would like to thank J.Anglin and J.P.Paz for useful conversations.

## References

- [1] R.Graham, D.E.Knuth, and O.Patashnik. *Concrete Mathematics*. Addison Wesley, 1994.
- [2] See A. K. Lenstra and H. W. Lenstra in Handbook of Theoretical Computer Science, ed. J. van Leeuwen, MIT Press/Elsevier, 1990. For an opposing argument, see: V. R. Pratt. Every Prime has a Succinct Certificate. *SIAM J. Comput.*, 4(1):214, 1975.
- [3] A. K. Lenstra and H. W. Lenstra, editors. *The Development of the Number Field Sieve.*, volume Lecture Notes in Mathematics 1554. Springer-Verlag, 1993.
- [4] P. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proc. 35th Annual Symposium on Foundations of Computer Science*. IEEE Press, Nov. 1994.

- [5] W. H. Zurek. *Physics Today*, 44:36, 1991.
- [6] W. H. Zurek. *Phys. Rev. D*, 24:1516, 1981, W. H. Zurek. *Phys. Rev. D*, 26:1862, 1982.
- [7] W. H. Zurek. In G.T. Moore and M.O.Scully, editors, *Frontiers of Nonequilibrium Statistical Physics*, New York, 1986. Plenum.
- [8] E. A. Lee and D. G. Messerschmitt. *Digital Communication*. Kluwer Academic Publishers, 1988.
- [9] S. Lloyd. *Science*, 261:1569, 1993.
- [10] David P. DiVincenzo. Two-Bit Gates are Universal for Quantum Computation. *Workshop on Quantum Computing and Communication, Gaithersburg, MD, August 18-19, 1994*.
- [11] I. L. Chuang and Y. Yamamoto. A Simple Quantum Computer. *Submitted to Phys. Rev. A*, 1994.
- [12] J. Cirac and P. Zoller. Quantum Computations with Cold Trapped Ions. *unpublished*, 1994.
- [13] R. Landauer. Is Quantum Mechanically Coherent Computation Useful? In D.H.Feng and B-L. Hu, editors, *Proc. of the Drexel-4 Symposium on quantum Nonintegrability – Quantum Classical Correspondence*, 1994.
- [14] W. G. Unruh. Maintaining coherence in Quantum Computers. *UBC preprint, hep-th/9406058*, 1994.
- [15] J. P. Paz. *unpublished*, 1994.

Figure 1: Probability distribution for the measurement of  $c$  in the state given in Eq.(3) with  $N = 21$ ,  $q = 128$ ,  $x = 5$ ,  $k = 3$ . The broadening of the peaks is a result of using discrete Fourier transform with  $q$  possible modes; a continuous Fourier transform would have given delta functions.

Figure 2: Effect of decoherence on the probability distribution for the measurement of  $c$ . The state given by Eq.(8) once  $a$  if Fourier transformed. The decoherence parameter Eq.(9) has been taken to be  $\xi = 0.1$ . The dotted line shows the good agreement of our constant-beta approximation, taking  $\beta = 0.58$ .

This figure "fig1-1.png" is available in "png" format from:

<http://arXiv.org/ps/quant-ph/9503007v1>



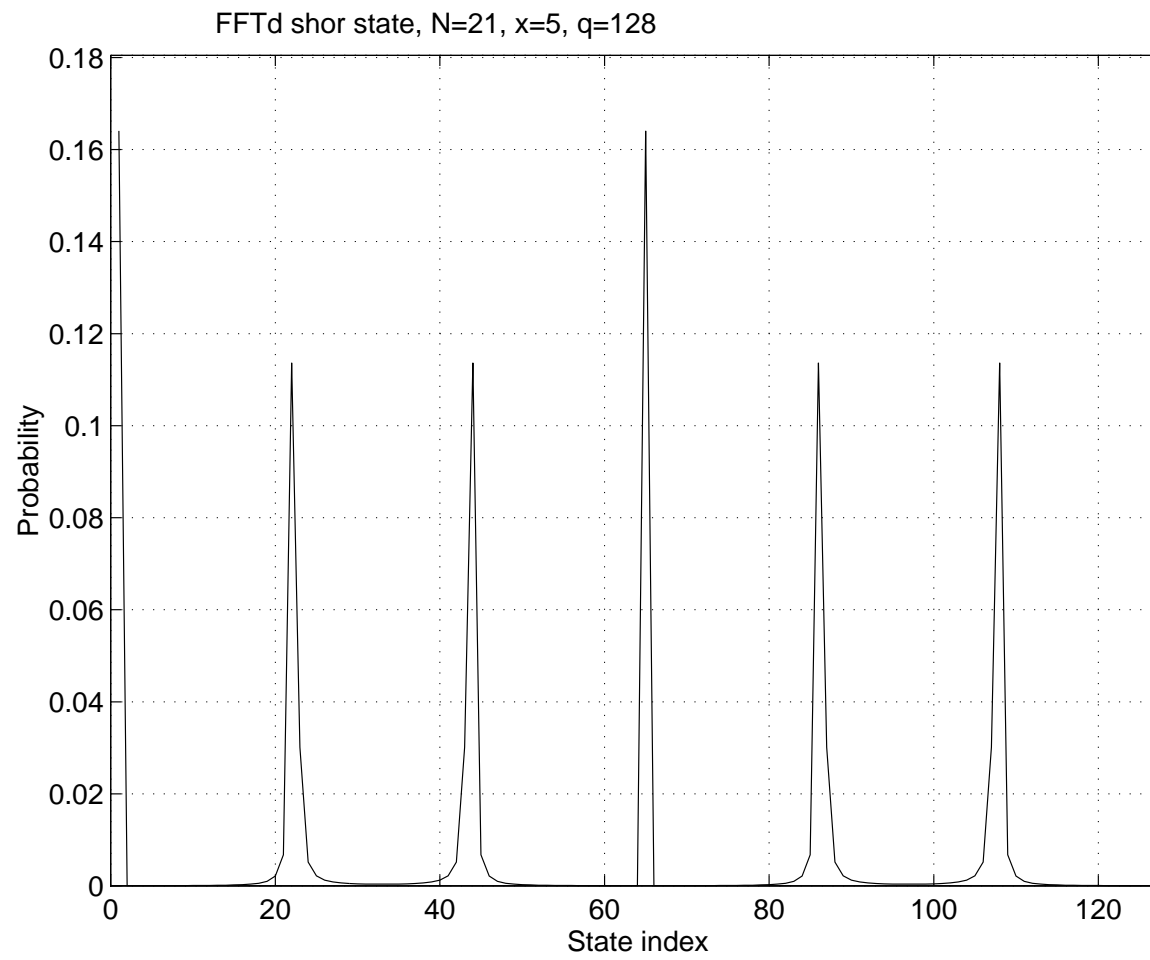


Figure 1

This figure "fig1-2.png" is available in "png" format from:

<http://arXiv.org/ps/quant-ph/9503007v1>

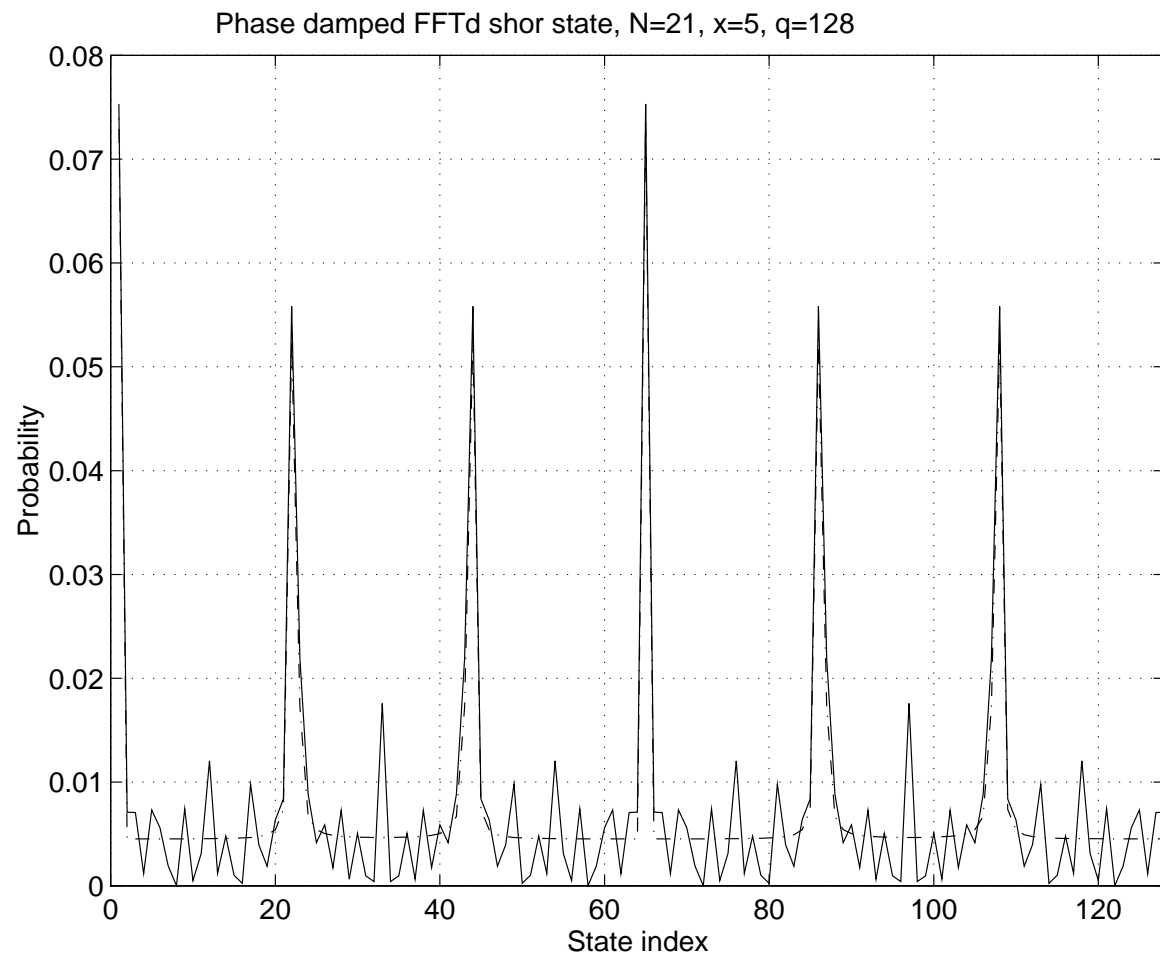


Figure 2